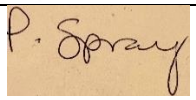
Online Safety Policy 2025-2026

Spurcroft Primary School & Nursery

This policy was approved at the meeting of the Governing Board in November 2025

This policy is due for review in November 2026

Headteacher	Sign & Date:	
Chair of Governing Board	Sign & Date:	

1. Introduction

This policy sets out Spurcroft Primary School & Nursery's approach to online safety, ensuring all members of the school community use digital technology safely, responsibly and ethically. It is written in line with Keeping Children Safe in Education 2025 (KCSIE 2025).

2. Purpose

- To protect all members of the school community from harm related to online activity and emerging technologies.
- To ensure the safe, responsible use of digital technology (devices, networks, online platforms) and the considered use of generative AI tools.
- To ensure that technology procurement, deployment and use are planned and monitored in line with national guidance and safeguarding responsibilities.
- To provide clear guidance on online safety, responsibilities and acceptable practice for staff, students and parents/carers.

3. Scope

This policy applies to:

- All staff, governors, volunteers, and students at the school.
- All devices and systems provided by the school (computers, tablets, iPads, mobile devices).
- Personal devices used to access school networks, platforms or for school-related use.
- All online platforms, internet access, email, social media and learning tools used by the school community.
- The use of generative AI tools by staff or students in the context of learning, teaching or assessment.

4. Roles and Responsibilities

4.1 Governing Board

- Ensures that an effective online safety policy is in place, reviewed regularly, and that it aligns with KCSIE and other DFE and Ofsted guidance.
- Oversees that appropriate filtering and monitoring systems are in place and managed effectively, as part of the technology planning process.

4.2 Headteacher/Designated Safeguarding Lead (DSL)

- Has overall responsibility for online safety and for ensuring the policy is implemented.
- Ensures that staff are trained, that incidents are reported appropriately, and that technology investment supports safe and effective provision.
- Leads responsibility for online safeguarding issues and incidents.
- Maintains up-to-date knowledge of online risks and technology developments.
- Works with the IT Subject Leads & IT Technician to ensure that safeguarding considerations are embedded in technology planning and filtering/monitoring systems.

4.3 IT Technician

- Ensures that the school's hardware and systems promote safety online
- Reports any concerns to the DSL.

4.4 IT Subject Lead

- Ensures that the school's curriculum promotes safety online, following the guidance in KCSIE.
- Reports any pupil safeguarding concerns to the DSL.
- Reports and hardware or filtering failures to the DSL and the IT Technician.

4.5 Staff

- Follow the school's Acceptable Use Policy (AUP).
- Model safe and responsible use of technology, following guidance from the DfE, Headteacher & IT Technician.
- Ensure they keep up to date with the latest guidance and advice.
- Understand the school filtering and monitoring systems, and their personal use of the staff proxy.
- Implement this policy in lessons or in activities where pupils or adults are using technology.
- Be vigilant for online safety issues and report concerns to the DSL or Deputy DSL.
- Take account of the DfE's generative AI guidance when using AI tools in their roles.

4.6 Students

- Follow the school's Pupil Acceptable Use Policy (AUP).
- Use devices and internet in a way that keeps themselves and others safe.
- Report concerns or inappropriate content to a teacher or trusted adult.

4.7 Parents/Carers

- Support and reinforce the school's online safety policy at home.
- Work with the school and their child to agree on safe usage of devices and online tools.
- Engage with guidance and training offered by the school.

5. Education and Training

- Students will receive age-appropriate education covering online safety, digital literacy, and an introduction to responsible use of AI.
- Staff will receive regular training on online safety risks, emerging technologies (including generative AI), curriculum implications, and their professional responsibilities.
- Parents/carers will be provided with guidance and resources regarding online safety at home, including emerging issues around generative AI.
- Technology planning will include provision for training, monitoring and safe integration of AI tools as per the "Plan technology for your school" guidance.

6. Acceptable Use

- All users must sign the appropriate Acceptable Use Policy (AUP) before accessing school devices or systems.
- Devices and networks must primarily be used for school-related work, teaching, learning and administration.
- Personal data, sensitive information, or student work should not be submitted to generative AI tools unless the tool and its usage have been formally approved by the school and align with data protection law and copyright requirements. (See section 12).

- Users must not deliberately bypass security settings or deploy unauthorised software or apps, including AI services, without approval.

7. Online Safety Risks

The school recognised the breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into the four areas of risk described in KCSIE 2025:

- **content:** being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.
- **contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **conduct:** online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and commerce: risks such as online gambling, inappropriate advertising phishing and or financial scams.

8. Monitoring and Filtering

- The school uses filtering and monitoring systems to restrict access to inappropriate content and to detect patterns of concern.
- These systems and the school's approach to technology are reviewed regularly and aligned with the "Plan technology for your school" guidance.
- Staff have training each year on how the filtering system and staff proxy settings work.
- They understand that their proxy login should not be given to others, and that pupils must NEVER be left alone with a device logged in on the staff proxy system.

9. Reporting and Responding to Incidents

- All online safety incidents, including misuse of AI tools, must be reported to the DSL immediately.
- The school will respond in line with its Safeguarding Policy and KCSIE 2025 obligations.
- Misuse of generative AI such as the input of personal or school data into AI will be treated as a serious matter and may lead to disciplinary measures, in accordance with school policy.
- The school will review incidents, update risk assessments and adjust technology use or training accordingly.

10. Use of Personal Devices

- As described in the school Code of Conduct for Staff and Volunteers, using mobile phones for personal use, in a pupil free area, during break times (such as in the staff

room) is acceptable. Using a phone in front of children, or for personal use during work time is not acceptable. If a mobile phone is needed for an acceptable reason, this should be discussed with the Headteacher.
- Other personal devices may only be used in school or for school systems with explicit permission and under the conditions set by the Headteacher.
- Staff must ensure personal devices used for school work are secure, data is protected, and unauthorised AI tools are not used for school or pupil data unless approved.

11. Remote Learning

- All remote learning must use school-approved platforms, accounts and follow the AUP.
- Students and staff must adhere to safe practices when using devices, internet and tools at home, including any AI tools – only approved tools may be used, and any data shared must comply with school policy and data protection law.
- Technology planning must account for remote learning, including safe access, monitoring and support for AI usage.

12. Generative Artificial Intelligence (AI) – Special Considerations

12.1 Understanding and Opportunities

- Generative AI refers to tools (e.g., large-language models like ChatGPT, Microsoft Copilot) that can create new content (text, images, audio, code) based on large data sets.
- The DfE states that when used safely and responsibly, generative AI has potential to support personalised learning, lesson planning, reducing teacher workload and tailored feedback.
- However, the DfE also highlights risks: inaccuracy, bias, copyright and intellectual property issues, data protection concerns, and the risk of misuse (for example students submitting AI-generated work as their own).

12.2 Approval

- Any use of generative AI by the school staff should be agreed by the Headteacher.
- Schools must ensure compliance with data protection legislation, copyright and intellectual property law when using AI tools.

12.3 Safe Supervision and Use

- Generative AI tools should not be used by pupils in school or by staff in front of pupils.
- Staff remain responsible for any content produced using AI tools — the output does not remove professional responsibility to check accuracy, suitability and appropriateness.

12.4 Education & Literacy

- Pupils will be supported to develop digital literacy skills including understanding what generative AI is, its benefits and limitations, the ethics around its use, how to identify AI-generated content, and how to use it responsibly.

13. Review

This policy will be reviewed annually, or sooner if:

- Statutory guidance (such as KCSIE) is updated.
- New technologies or platforms (such as generative AI tools) are introduced or become mainstream.
- A significant online safety incident involving AI occurs.
- The school's technology plan is updated in line with national guidance.

References:

- Keeping Children Safe in Education 2025 (KCSIE 2025)
- Generative artificial intelligence (AI) in education (DfE)
- UK Safer Internet Centre – Online Safety Resources